

~~c) a step of generating a digital signature based upon the first information and the secret key information.~~

~~27. A computer readable memory which cooperates with a data processor and an information input unit to carry out:~~

~~a) a step of inputting first information;  
b) a step of storing secret key information which is fed from an external device; and  
c) a step of generating a digital signature based upon the first information and the secret key information.--~~

REMARKS

A Petition pursuant to 37 CFR § 1.136(a) and the fee required by 37 CFR § 1.17(a)(3) are submitted herewith. Accordingly, the due date for response to the Official Action mailed (January 7, 1999 (Paper No. 1) is now July 7, 1999.

The Abstract has been amended to describe the invention more fully.

Claim 8 has been amended to correct a misspelling.

Claim 11 has been amended to correct an antecedent basis error and to correct a misspelling.

Claims 1-4 were rejected under 35 U.S.C. § 102(b) as being unpatentable by Friedman (IEEE Vol. 39).

Independent claim 1 has been amended to set forth more clearly the feature which distinguishes this invention from the prior art, namely:

"means for storing secret key information which is fed from an external device".

The significance of this is that the device may be used by any of several users who have an external device, for example a card, from which their own secret key may be input and stored. When the user inputs his or her secret key information from the external device, together with input information, the authenticity of the input information, i.e., assurance that it came from the user without change, can be verified.

The prior art, including the cited reference to Friedman fails to disclose the idea of a means for storing secret key information which is fed from an external device. Friedman only discloses a camera which contains its own secret key. While this allows one to ascertain that an image came from the particular camera, it does not give the receiver any assurance regarding the user of the camera.

The present invention, on the other hand, by providing a means for storing secret key information which is

fed from an external device, allows any person who has an external device, for example a card, from which his or her secret key can be fed to and stored in the camera or other device, enables any number of users to transmit information to a receiver; and the receiver may be assured that the information actually came from the particular individual who purported to send it.

Friedman gives no disclosure or suggestion of providing input of secret key information from an external device. Instead, Friedman only discloses a camera in which a secret key is imbedded.

In view of the foregoing it is submitted that claim 1 as now amended patentably distinguishes over Friedman and is allowable.

Claims 2-5 are dependent on claim 1 and incorporate its above discussed distinguishing recitations. Accordingly, these claims patentably distinguish over Friedman for the same reasons given above. In addition, the specific structures defined by these dependent claims provide additional advantages, as can be seen from the specification, as well as additional novelty; and for these reasons also, claims 2-5 are allowable.

Claims 6-9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman.

Independent claim 6 as now amended, specifies:

"means for storing secret information which is fed from an external device".

In addition, claim 6 adds the further feature of compression of the first information and for generating a distinguishing information based on the compressed information. Claim 6 thus now recites the same features which distinguish claim 1 from Friedman, as discussed above. It is submitted therefore, that claim 6, as now presented, patentably distinguishes over Friedman and is allowable.

Claims 7-9 are dependent on claim 6 and patentably distinguish from Friedman for the same reasons and for the further reasons that the specific structures set forth in these dependent claims provide additional advantages, as can be appreciated from the specification, as well as additional novelty.

Claims 10-13 were rejected under 35 U.S.C. § 102(b) or 103(a) (claim 13) as being anticipated by or unpatentable over Friedman.

Claim 10 has been amended to specify:

"a memory for storing secret information which is fed from an external device".

As discussed above, Friedman does not disclose or suggest a memory which stores secret information which is fed from an external device. Accordingly claim 10 patentably distinguishes over Friedman for the reasons given above in regard to claim 1.

Claims 11-13 are dependent on claim 10 and are allowable for the same reasons. In addition, the specific structures defined by these dependent claims provide additional advantages, as can be appreciated from the specification, as well as additional novelty; and for these reasons also, claims 11-13 are allowable.

Claims 14-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Friedman.

Claim 14 has been amended to specify:

a second terminal device for having a memory for storing secret information which corresponds to a user".

As discussed above in regard to claims 1, 6 and 10 the Friedman reference fails to disclose or suggest a device which stores secret information corresponding to a user. Instead, the Friedman device only stores information relating to a specific camera, which insofar as the receiver knows, could have been operated by anyone. Therefore the receiver has no idea who has been operating the camera.

With the present invention the user is always identified to the receiver and therefore the receiving party can always be assured that the information has come from the person who purports to have sent it.

In view of the foregoing it is submitted that claim 14 as now amended patentably distinguishes over Friedman and is allowable.

Claims 15-20 are dependent on claims 14 and patentably distinguish over Friedman for the reasons given above. These dependent claims also define specific structures which provide additional advantages, as can be appreciated from the specification, as well as additional novelty. For these reasons also, claims 150-20 are allowable.

Claims 21-25 have been cancelled.

New claims 26 and 27 have been added to assure a fuller measure of protection for applicant's invention. Claims 26 and 27 are based on claim 1 and set forth the same distinguishing recitations discussed above in regard to claim 1. Claim 26 is a method claim corresponding to claim 1; and claim 27 is directed to a computer readable memory which cooperates with a data processor and an information input unit for performing the steps of inputting information,

storing a secret key which is fed from an external device and for generating a digital signature based on the information and the secret key. As pointed out above, Friedman does not disclose or suggest an arrangement for storing secret key information which is input from an external device.

For the foregoing reasons, new claims 26 and 27 patentably distinguish over Friedman and are also allowable.

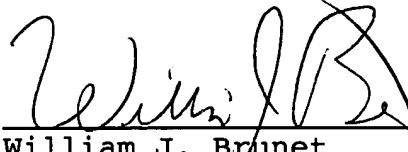
The other references cited in the Official Action, which were not applied to the claims, have been considered; and it is agreed that these other references do not disclose or suggest the above discussed distinguishing features of applicant's invention.

In view of the foregoing, it is submitted that all of the claims now present in the subject application are allowable. Further consideration by the Examiner and allowance of the application is respectfully requested.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All

correspondence should continue to be directed to our below  
listed address.

Respectfully submitted,



\_\_\_\_\_  
William J. Brunet  
Attorney for Applicant  
Registration No. 20,452

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

NYMAIN#13458v1